

Howard Shrobe

Program Manager, Information Innovation Office

Secure Computer Systems

DARPA Cyber Colloquium
Arlington, VA

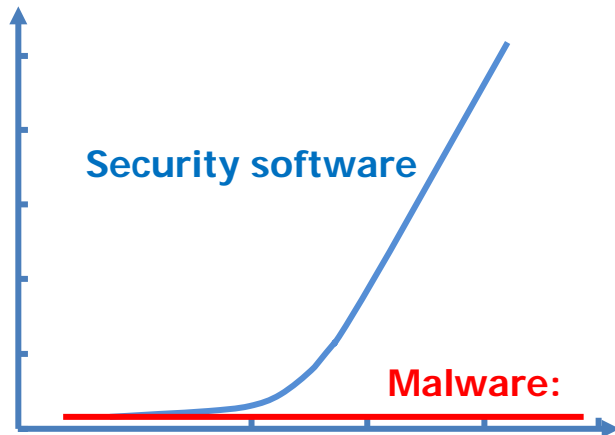
November 7, 2011



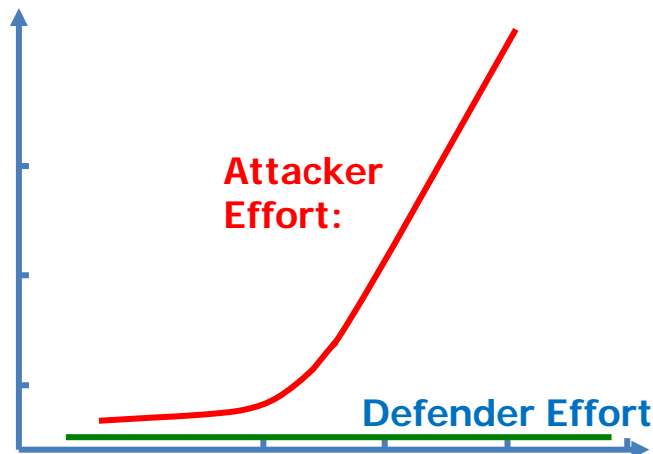
Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 07 NOV 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Secure Computer Systems				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Advanced Research Projects Agency (DARPA), Information Innovation Office, 3701 North Fairfax Drive, Arlington, VA, 22203-1714				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 15	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Today's Practice P4: Perimeter Protection, Patch & Pray isn't Convergent with The Threat



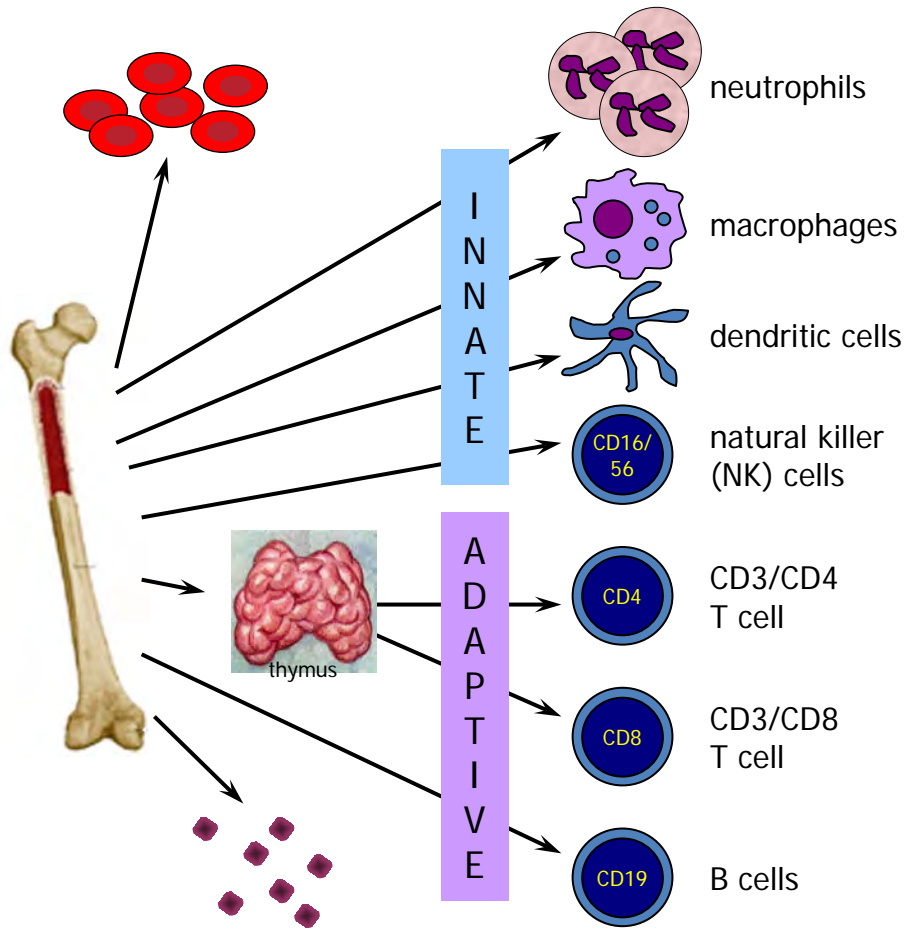
- It's not about better firewalls
- It's not about better virus detection
- It's not about better intrusion detection
- It's not about better programmer practices



**It's about learning from biology
and societies how to design
secure, adaptive and resilient
systems.**



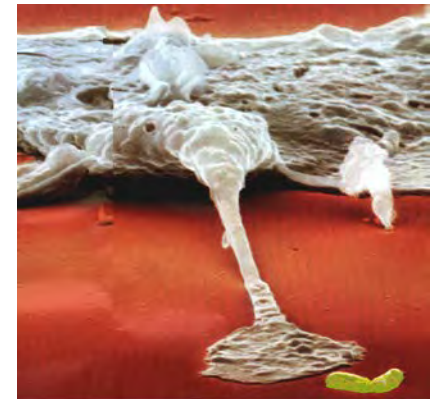
Humans Have Two Immune Systems: Innate and Adaptive



Fast, but inflexible, covers fixed sets of pathogen that are always present. Supports the adaptive immune system.



Slower, learns to recognize new sets of pathogens, distinguishes self from non-self, retains memory to guard against future attacks.



At least 20 – 30% of the body's resources are involved in constant surveillance and containment.



Three Big Problems

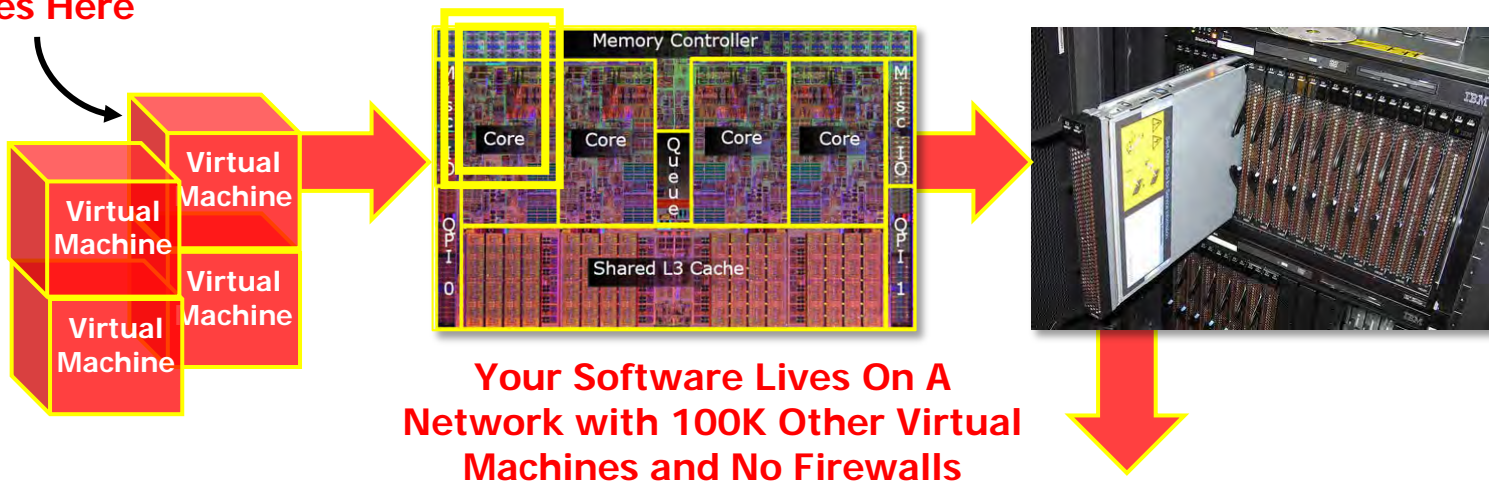
1. Systems can be easily penetrated
2. Once penetrated, cleanup is prohibitively expensive, time-consuming, and unpredictable
3. If one system can be penetrated, then nearly all of them can



Mission-oriented Resilient Clouds

Using the power of a computational community to protect massively shared computational infrastructure

Your Software Lives Here



Modular Data Center Containers



Blade Server Racks



Blade Server Network



Resilient Clouds: A Community that uses the Network as a *Defensive Amplifier*

TODAY

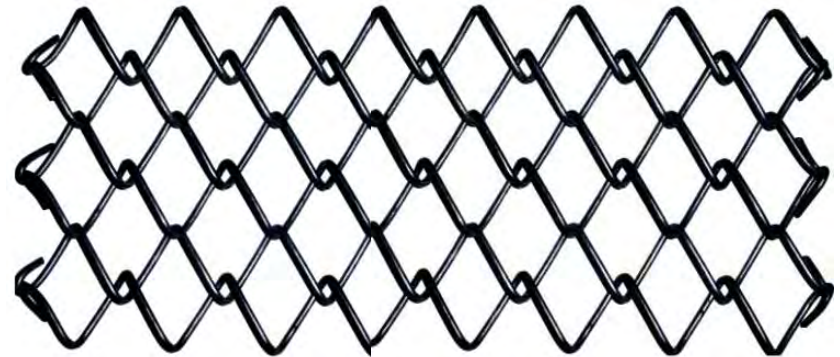
Acting as individuals makes the enterprise weaker than the sum of its parts



- "Box" Oriented
- Vulnerable Components
- Static Sitting Duck
- Shared Vulnerabilities
- Implicit Trust is Amplifier

RESILIENT CLOUDS (CRASH++)

Acting as a community makes the enterprise stronger than the sum of its parts



- Mission Optimized
- CRASH-worthy components
- Moving Target
- Resilience through Diversity
- Collective Diagnosis is Damper



Resilient Clouds Technology Areas

Combined Goal of CRASH
& Resilient Clouds

Cyber-Mission Resilience

Resilient Clouds Technologies

Mission-Aware
Networking

Optimizing Mission
and Resources

Innate Distributed
Defense

Shared Situational Awareness,
Trust Modeling, and Diagnosis

Manageable & Taskable
Diversity

CRASH Technologies

Innate Immunity

Adaptive Immunity

Manageable Diversity

For more info see: <http://tinyurl.com/68w9w9pf>

➔ Information flow
➡ Control flow



Secure Computer Systems

CRASH

Clean-slate design of **R**esilient, **A**daptive, **S**ecure **H**osts

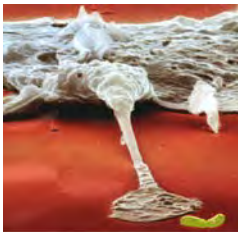


CRASH Applies Biological Principles to Computation



Innate Immunity:

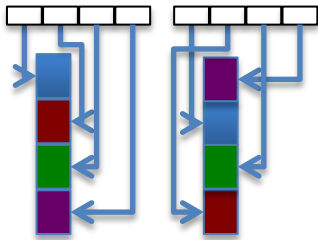
New hardware & operating system architectures that eliminate all common technical vulnerabilities



Adaptive Immunity

Middleware that:

- Diagnoses root causes of vulnerabilities and builds situational assessment
- Quickly adapts & reconfigures
- Learns from previous attacks and gets better at self-protection



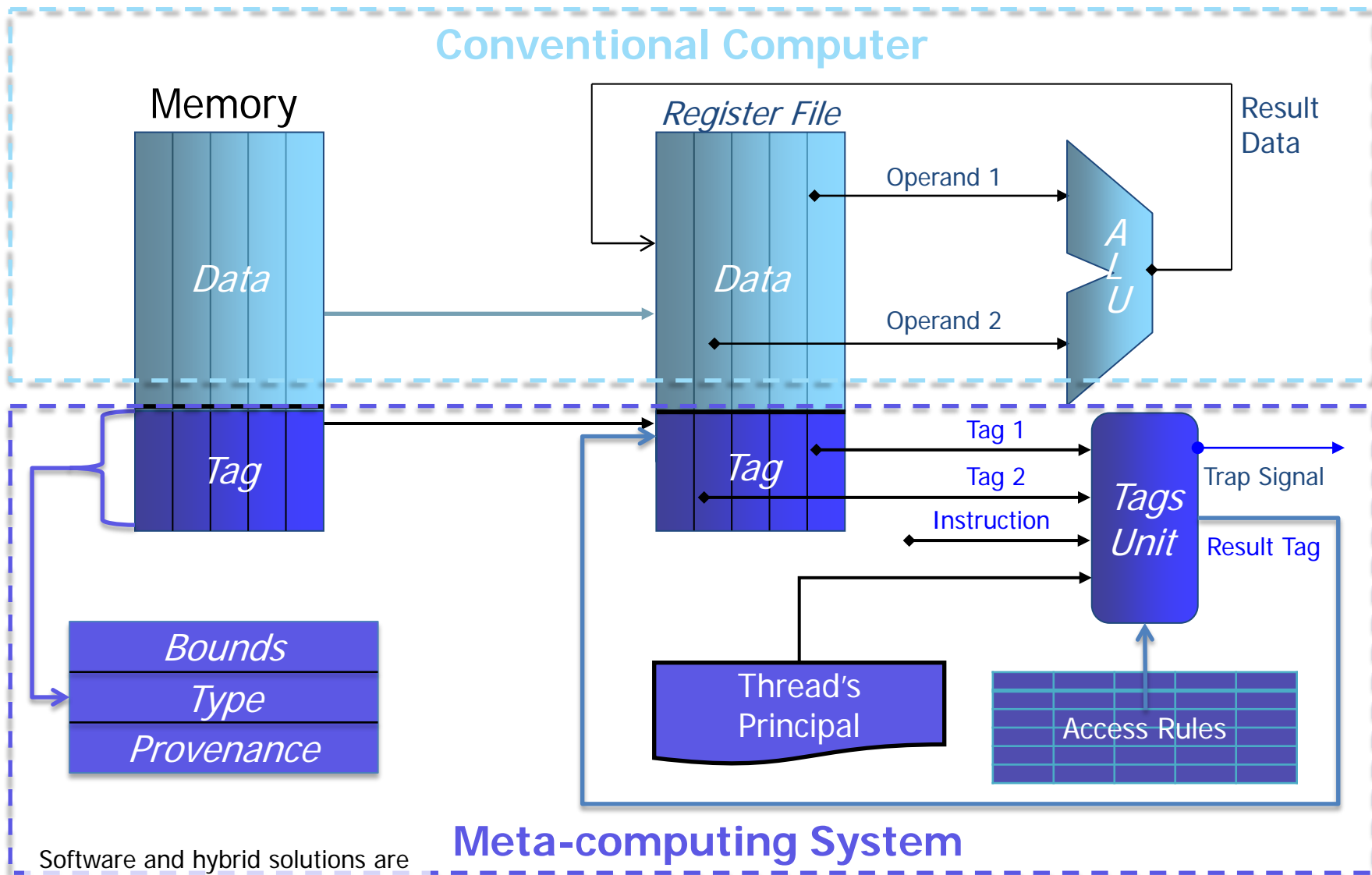
Population Diversity

Computational techniques that:

- Increase entropy in time and space
- Make every system unique
- Raise work factor of attacker for each system



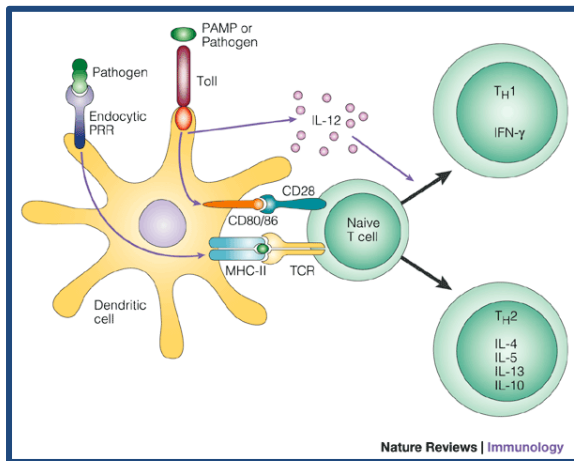
Innate Immunity: An Example Hardware Solution



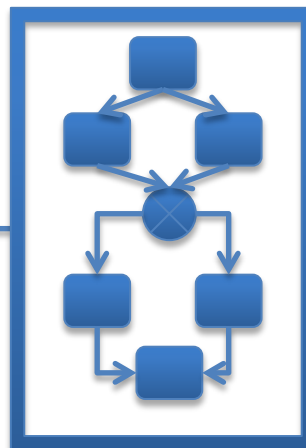
Software and hybrid solutions are also possible (e.g. PROCEED)



Adaptive Immunity

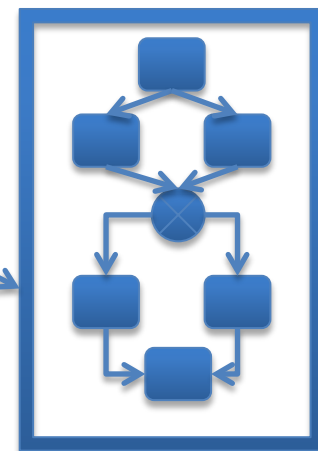


System Model



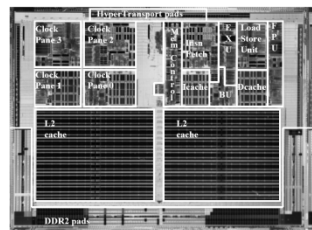
4. System model is adapted with new attack-specific detector

3. System model is used to perform diagnosis (e.g. localization and characterization)



5. Adaptive immune system synthesizes plan to get around problem and patch to remove specific vulnerability

2. Software system analog of adaptive immune system is signaled

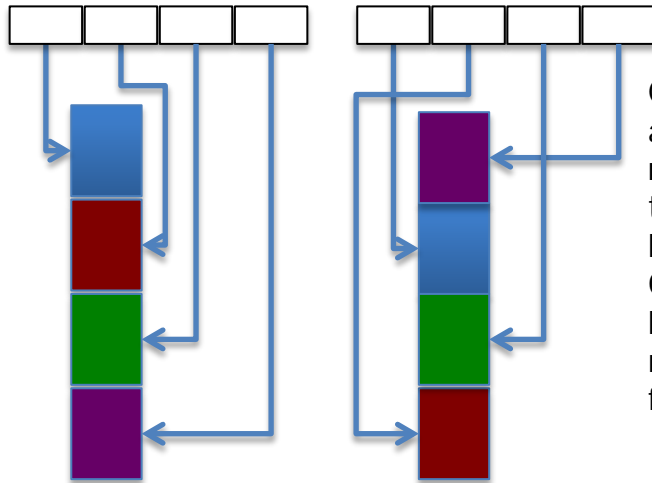


1. Hardware analog of innate immune system detects anomaly



Dynamic Diversity Makes a Single Host Different from Moment to Moment

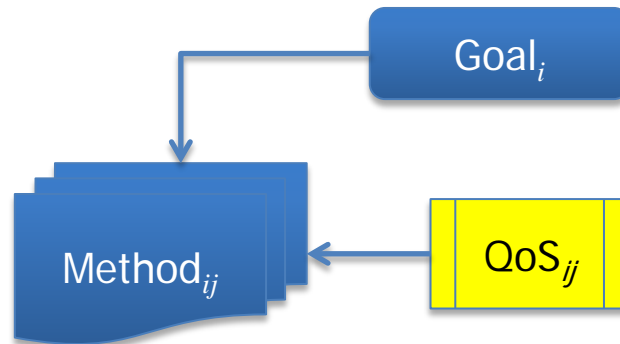
Address Space Randomization



Code and/or data blocks are periodically repositioned in memory so that attacker has to work harder to find a target. Garbage-collected memory has the property inherently, new methods may optimize for increased entropy.

Functional Redundancy & Decision Theoretic Dispatch

There are multiple methods for achieving each goal ("n-version programming"). Each distinct method has different qualities of service. Method selection is driven both by preferences over QoS and by need for unpredictability.



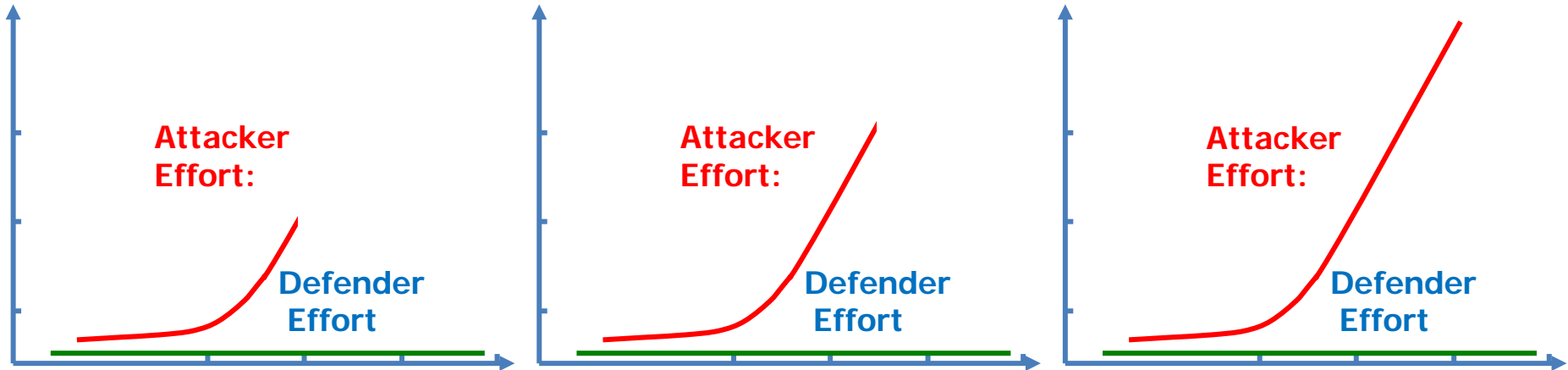
Instruction Set Randomization

Disk	Memory	ICache
Instruction-1	Encrypted-1	Instruction-1
Instruction-2	Encrypted-2	Instruction-2
Instruction-3	Encrypted-3	Instruction-3
Instruction-4	Encrypted-4	Instruction-4
Instruction-5	Injected-1	Encrypted-1
Instruction-6	Injected-2	Encrypted-1
	Encrypted-5	Instruction-5
	Encrypted-6	Instruction-6

Code is encrypted as it enters memory and Decrypted as it enters the instruction cache (or translation buffer). Injected code in native instruction set is then encrypted and not executable. Encryption key can be varied by process and time.



Turn the Tables: Make The Attacker Do The Work



Innate Immunity

- Novel Hardware
- Separation OS's
- Information Flow
- Formal Methods

Adaptive Immunity

- Policy Weaving
- Automatic Patching
- Selective Playback
- Symbiotes

Dynamic Diversity

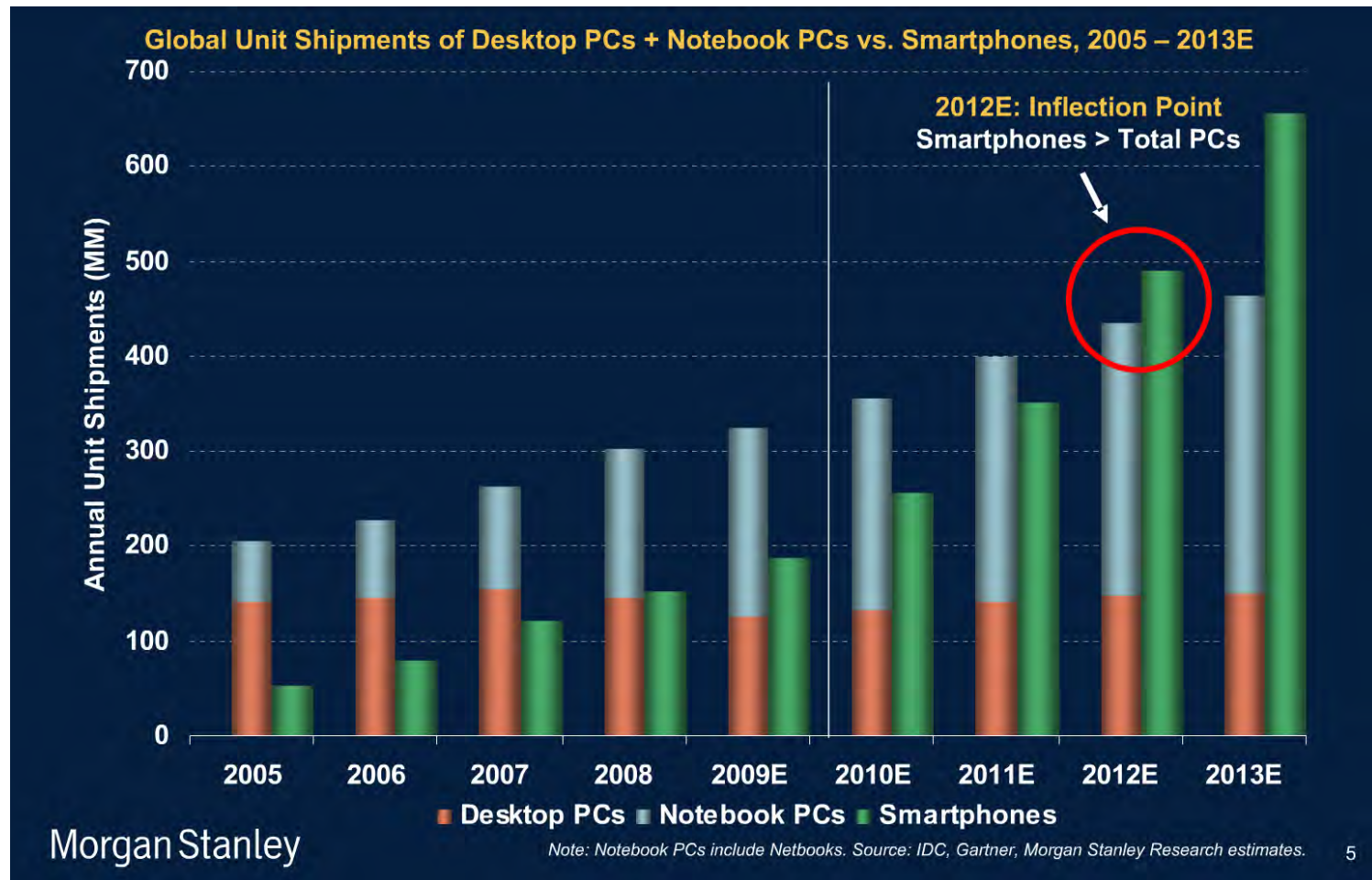
- Compiler generated Diversity
- Algorithmic Diversity
- Instruction Set Randomization



An opportunity...

Smartphone > PC shipments within 2 years

Implies very rapid, land grab evolution of internet access





Our goal...

...is to get CRASH & MRC technologies into *your* machines.

- If you make computers, operating systems, middleware...
- If you use these and can influence the people who make them
- If you think there's a great startup opportunity

- Then we want to talk with you about how to transition our technologies into the real world.
- Contact us at CrashInquiries@darpa.mil